SC-402 - Cryptography

Page No. : 1

Date :

Homework - 3

Id - 201901100

Name - Shubham Patel

[1] Here

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_2 + x_3 + x_4 + x_5 &= 1 \\ x_3 + x_4 + x_5 + x_6 &= 0 \\ x_4 + x_5 + x_6 + x_7 &= 1 \end{aligned} \longrightarrow \begin{cases} x_4 = x_2 + x_3 + x_5 \\ x_5 = 1 + x_1 \\ x_6 = 1 + x_2 \\ x_7 = 1 + x_3 \end{cases}$$

So, we get,

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	1	1	1
0	0	1	1	1	1	0
0	1	0	1	1	0	1
0	1	1	0	1	1	0
1	0	0	1	0	1	1
1	0	1	1	0	1	0
1	1	0	0	0	0	1
1	1	1	1	0	0	0

[2] Assume $m \geq 2$,

(a) Suppose 'a' is even,
so $a\,2^{m-1} \equiv 0 \pmod{2^m}$
also $2^{2m-2} \equiv \pmod{2^m}$

Define $x' = x + 2^{m-1} \bmod 2^m$;

so, $h(x') = (x+2^{m-1})^2 + a(x+2^{m-1}) + b \bmod 2^m$
$= x^2 + 2^m x + 2^{2m-2} + ax + a\cdot 2^{m-1} + b \bmod 2^m$
$= x^2 + ax + b \bmod 2^m$
$= f(x)$

Suppose 'a' is odd,
Define $x' = -x - a$
we have;
$h(x') = (-x-a)(-x) + b \bmod 2^m$
$= (x+a)(x) + b \bmod 2^m$
$= h(x)$

(b) Define $x' = x + 2^m \bmod 2^m$.
Then, $x' \neq x$, and $h(x') = h(x)$

[3] Here we have, $x = x' \| x''$
let $x_0 \in \{0,1\}^m$ and $x_0 \neq 0$

Define, $x_1' = x' \oplus x_0$, $x_1'' = x'' \oplus x_0$
and $x_1 = x_1' \oplus x_1''$.
Then $x \neq x_1$ and $h(x) = h(x_1)$

[4]

(a) Assume, we found a collison for h_2. so $h_2(x) = h_2(x')$ where $x \neq x'$.
- denote. $x = x_1 \| x_2$ and $x' = x_1' \| x_2'$
- Suppose that $h(x_1) \neq h_1(x_1')$. Then
$h_1(x_1) \| h_1(x_2) \neq h_1(x_1') \| h_1(x_2')$.
And $h_1(h_1(x) \| (h_2(x_2)) = h_2(h_2(x_1')) \| h_1(x_2')$

- Therefore, we found collison for h_1.

- If $h_1(x_2) \neq h_1(x_2')$, Then we have a collison for h_1.
By similar assumption, $h_1(x_1) = h_1(x_1')$ and $h_1(x_2) = h_1(x_2')$ because $x \neq x'$, it follows $(x_1, x_2) \neq (x_1', x_2')$.
- We can always found collison for h_1, given collison for h_2.

(b) Suppose, we found a collison for h_i, because $h_i(x) = h_i(x')$ where $x \neq x'$.

- Denote, $x = x_1 \| x_2$ and $x' = x_1' \| x_2'$
- Suppose that $h_{i-1}(x_1) \neq h_{i-1}(x_1')$ then $h_{i-1}(x_1) \| h_{i-1}(x_2) \neq h_{i-1}(x_1') \| h_{i-1}(x_2')$ and $h_i(h_{i-1}(x_1) \| h_{i-1}(x_2)) = h_i(h_{i-1}(x_1') \| h_{i-1}(x_2'))$
- So we found collison for h_i.
- If $h_{i-1}(x_2) \neq h_{i-1}(x_2')$. Then we have a collison for h_i by similar assumption.
- Therefore we can assume that $h_{i-1}(x_1) = h_{i-1}(x_1')$ and $h_{i-1}(x_2) = h_{i-1}(x_2')$ because $x \neq x'$. It follows $x_1 \neq x_1'$ or $x_2 \neq x_2'$.
- We always can find a collison for at least one of h_i or h_{i-1}, given collison for h_i.